数理解析研究所講究録
603 巻 1987 年 21-34

Niedere Potenzen von Ringklasseneinheiten

Reinhard Schertz, Universität Augsburg

1. Ergebnisse

Sei Σ ein imaginär-quadratischer Zahlkörper und Ω_f, $f \in \mathbb{N}$, der Ringklassenkörper modulo f über Σ. Dann kann man bekanntlich mit Hilfe der für ein komplexes Gitter $\mathfrak{w}$ definierten Diskriminante

$$(1.1) \qquad \Delta(\mathfrak{w}) = \left(\frac{2\pi}{\omega_2}\right)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24},$$

$$\mathfrak{w} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad \mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0, \quad q = \exp\left(2\pi i \frac{\omega_1}{\omega_2}\right)$$

in den Teilkörpern von Ω_f vollständige Einheitsgruppen konstruieren, deren Index in der vollen Einheitengruppe des betreffenden Körpers ähnlich wie für reelle Kreiskörper im wesentlichen gleich der Klassenzahl ist. Diese Beziehung ist sehr nützlich. So lassen sich zum Beispiel durch Untersuchung der beteiligten Δ-Werte Teilbarkeitsaussagen für Klassenzahlen herleiten (vgl. [12]). Eine andere Anwendung besteht darin, daß man analog zu dem Algorithmus von Gras [2] im Kreiskörperfall mit Hilfe geeigneter Δ-Werte Grundeinheiten und Klassenzahl der betreffenden Körper berechnet. Diese zuerst von Kronecker [4] zur Lösung der Pellschen Gleichung benutzte Methode ist in jüngster Zeit mit Erfolg für die Körper vom Grade 3, 4 und 6 durchgeführt worden (vgl. [8, 9,10]).

Zur Konstruktion der genannten Einheiten sei

$\mathcal{O}_f$ die Ordnung zum Führer f in Σ,
I_f die Gruppe der eigentlichen Ideale von $\mathcal{O}_f$,
H_f die Untergruppe der Hauptideale in I_f,
$\mathfrak{K}_f = I_f/H_f$ die Idealklassengruppe von $\mathcal{O}_f$,
$\sigma : \mathfrak{K}_f \longrightarrow \mathrm{Gal}\,(\Omega_f/\Sigma)$ der kanonische Isomorphismus.

Bekanntlich gilt dann

$$(1.2) \qquad \frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{b})} \in \Omega_f \quad \text{für } \mathfrak{a}, \mathfrak{b} \in I_f ,$$

und nach [15] wird Ω_f im Fall $\mathfrak{a}H_f \neq \mathfrak{b}H_f$ über Σ sogar durch diese Zahl erzeugt. Ihre Konjugierten sind gegeben durch

$$(1.3) \qquad \left(\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{b})}\right)^{\sigma(\mathfrak{k})} = \frac{\Delta(\mathfrak{a}\mathfrak{r}^{-1})}{\Delta(\mathfrak{b}\mathfrak{r}^{-1})}, \quad \mathfrak{a}, \mathfrak{b} \in I_f, \quad \mathfrak{k} \in \mathfrak{K}_f, \quad \mathfrak{r} \in \mathfrak{k} .$$

Die Faktorisierung dieser Zahl ist nach [1] vollständig bekannt, so daß man durch geeignete Produkte Einheiten konstruieren kann.

Für die oben genannten Problemstellungen sind dabei die durch

$$(1.4) \qquad \varepsilon(\mathfrak{k},\mathfrak{f}) = \left(\frac{\Delta(\mathfrak{a})}{\Delta(\mathcal{O}_f)}\right)^{\sigma(\mathfrak{f})-1} = \frac{\Delta(\mathfrak{a}\bar{\mathfrak{b}})\,\Delta(\mathcal{O}_f)}{\Delta(\mathfrak{a})\;\Delta(\bar{\mathfrak{b}})}$$

$$\text{mit} \quad \mathfrak{k},\mathfrak{f} \in \mathfrak{K}_f,\ \mathfrak{a} \in \mathfrak{k},\ \mathfrak{b} \in \mathfrak{f}$$

und dem zu $\mathfrak{b}$ konjugiert komplexen Ideal $\bar{\mathfrak{b}}$ definierten Einheiten besonders gut geeignet [3, 5, 8, 9, 10, 11, 12] . Hierbei werden sehr oft zu (1.2) und (1.3) analoge Informationen über die 24-ten Wurzeln der $\varepsilon(\mathfrak{k},\mathfrak{f})$ benötigt. So hängen zum Beispiel die in [12] bewiesenen Teilbarkeitsbeziehungen entscheidend von solchen Aussagen ab, und auch bei der o. g. Klassenzahl- und Einheitenberechnung sind diese nützlich, weil man so die mit Hilfe der $\varepsilon(\mathfrak{k},\mathfrak{f})$ konstruierten Einheitengruppen vergrößern kann.

Im Falle $\mathfrak{k} = \mathfrak{f}$ wurde die Frage nach den von den 24-ten Wurzeln erzeugten Körpern bereits vollständig in [12] beantwortet. In den anderen Fällen sind in [3, 5] recht komplizierte hinreichende Bedingungen angegeben worden unter denen $\varepsilon(\mathfrak{k},\mathfrak{f})$ die 24-te Potenz einer Zahl in Ω_f ist. Im Satz (1.3) der vorliegenden Arbeit werden nun in allen Fällen die durch die 24-ten Wurzeln erzeugten Körper bestimmt. Der Beweis benützt ähnlich wie in [12] die singulären Werte von $\gamma_2 = \sqrt[3]{j}$ und $\gamma_3 = \sqrt{j-12^3}$ und ist erheblich einfacher als die in [3, 5] verwendeten Schlußweisen. Darüber hinaus ergibt sich auf diesem Wege zugleich in expliziter Form die Aktion der Galoisgruppe auf den Wurzeln, was insbesondere für numerische Zwecke sehr nützlich ist.

Zur Beschreibung der 24-ten Wurzeln aus $\varepsilon(\mathfrak{k},\mathfrak{f})$ wählen wir in $\mathfrak{k}$ und $\mathfrak{f}$ reguläre ganze Ideale $\mathfrak{a}$ und $\mathfrak{b}$,

$$(1.5) \qquad \mathfrak{a} = \mathfrak{p}_f = \mathfrak{p} \cap \mathcal{O}_f \ , \quad \mathfrak{b} = \mathfrak{q}_f = \mathfrak{q} \cap \mathcal{O}_f$$

mit ganzen primitiven zueinander teilerfremden und zu $6f$ primen Idealen $\mathfrak{p}$ und $\mathfrak{q}$ von $\mathcal{O}_1$ der Norm p bzw. q . In $\mathcal{O}_f$ gibt es dann eine $\mathbb{Z}$-Basis der Form

$$(1.6) \qquad \begin{aligned} \mathcal{O}_f &= [1,\alpha] \quad \text{mit} \\ \mathfrak{a} &= [p,\alpha] \quad , \ \mathfrak{b} = [q,\alpha] \quad \text{und} \\ \mathfrak{a}\bar{\mathfrak{b}} &= [pq,\alpha] \quad . \end{aligned}$$

Letzteres folgt aus der Tatsache, daß $\mathfrak{p}$ und $\mathfrak{q}$ teilerfremd sind. Bezeichnet d_Σ die Diskriminante von Σ , so kann dabei α wegen $(6, pq) = 1$ durch

$$(1.7)\qquad \begin{array}{lll} \mathrm{Spur}\,(\alpha) \equiv 0(3) & & \\ \mathrm{Spur}\,(\alpha) \equiv 0(4) & , & \text{falls } d_\Sigma \equiv 0(2) \\ \mathrm{Spur}\,(\alpha) \equiv 1(4) & , & \text{falls } d_\Sigma \equiv 1(4) \end{array}$$

normiert werden. Dann ist

$$(1.8)\qquad \varepsilon(\mathfrak{k},\mathfrak{f}) = \left(\frac{\eta(\frac{\alpha}{pq})\ \eta(\alpha)}{\eta(\frac{\alpha}{p})\ \eta(\frac{\alpha}{q})}\right)^{24}$$

mit der Dedekindschen η-Funktion

$$(1.9)\qquad \eta(z) = q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)\ ,\quad q = e^{2\pi i z}\ .$$

Wir setzen

$$(1.10\qquad E(\mathfrak{a},\mathfrak{b}) := \frac{\eta(\frac{\alpha}{pq})\ \eta(\alpha)}{\eta(\frac{\alpha}{p})\ \eta(\frac{\alpha}{q})}\ ,$$

wobei die rechte Seite tatsächlich nur von den Idealen $\mathfrak{a}$ und $\mathfrak{b}$ abhängt. Dies folgt aus der Transformationsformel (2.2) und der Tatsache, daß α durch (1.6) und (1.7) bis auf ein ganzrationales Vielfaches von $12pq$ eindeutig bistimmt ist. Alledings ist $E(\mathfrak{a},\mathfrak{b})$ im allgemeinen keine Invariante der Klassen $\mathfrak{k}$ und $\mathfrak{f}$ mehr. Mit diesen Bezeichnungen gilt

<u>**Satz (1.1)**</u> Seien $\mathfrak{a},\mathfrak{b}$ wie in (1.5) und $\mathfrak{a} \neq \bar{\mathfrak{b}}$. Dann gilt

1) $$\Omega_f(E(\mathfrak{a},\mathfrak{b})^8) = \begin{cases} \Omega_{3f} & \text{falls } 3 \mid f^2 d_\Sigma \text{ und } N(\mathfrak{a}) \equiv N(\mathfrak{b}) \equiv -1(3) \\ \Omega_f & \text{sonst}\ . \end{cases}$$

2) $$\Omega_f(E(\mathfrak{a},\mathfrak{b})^3) = \begin{cases} \Omega_{2f}, & \text{falls } 2 \mid f^2 d_\Sigma \text{ und } N(\mathfrak{a}) \equiv N(\mathfrak{b}) \equiv -1(4) \\ \Omega_f & \text{sonst.} \end{cases}$$

Dabei bezeichnet $N(\mathfrak{a}) = [\ \mathcal{O}_f : \mathfrak{a}] = p$ und $N(\mathfrak{b}) = q$ die Idealnorm von $\mathfrak{a}$ und $\mathfrak{b}$, und es gilt $[\Omega_{3f} : \Omega_f] = 3$, $[\Omega_{2f} : \Omega_f] = 2$ in den entsprechenden Fällen.

3) Ist $E(\mathfrak{a}',\mathfrak{b}')$ eine weitere solche Einheit, so gilt für $t = 8,3$:

$$\Omega_f(E(\mathfrak{a},\mathfrak{b})^t) = \Omega_f(E(\mathfrak{a}',\mathfrak{b}')^t) \Rightarrow \left(\frac{E(\mathfrak{a}',\mathfrak{b}')}{E(\mathfrak{a},\mathfrak{b})}\right)^t \in \Omega_f\ .$$

Die Konjugierten der Zahlen $E(\mathfrak{a},\mathfrak{b})$ berechnen sich aus

Satz (1.2) Sei $\mathfrak{f}_0 \in \mathfrak{K}_f$ und $\mathfrak{b}_0 = \mathfrak{q}_0 \cap \mathcal{O}_f \in \mathfrak{f}_0$ mit einem ganzen zu $\bar{\mathfrak{q}}\mathfrak{q}$ und zu 6f primen primitiven Ideal $\mathfrak{q}_0$ von $\mathcal{O}_1$ der Norm q_0. Dann kann α so gewählt werden, daß auch $\bar{\mathfrak{b}}_0 = [q_0, \alpha]$ ist, und es gilt dann

$$E(\mathfrak{a},\mathfrak{b})^{\sigma(\mathfrak{f}_0)} = \frac{\eta(\frac{\alpha}{pqq_0})\ \eta(\frac{\alpha}{q_0})}{\eta(\frac{\alpha}{pq_0})\ \eta(\frac{\alpha}{qq_0})} .$$

Um Satz (1.1) auf die Einheiten $\varepsilon(\mathfrak{k},\mathfrak{f})$ anwenden zu können, benutzen wir die aus der Geschlechtertheorie bekannte Tatsache (vgl. auch [12]), daß im Fall $\sqrt{-3} \in \Omega_f$ das Legendresymbol $(\frac{-3}{N(\mathfrak{a})})$ für alle gemäß (1.5) normierten Vertreter einer Idealklasse $\mathfrak{f} \in \check{\mathfrak{K}}_f$ denselben Wert annimmt und somit vermöge

$$(1.11) \qquad \chi_{-3}(\mathfrak{f}) := (\frac{-3}{N(\mathfrak{a})}) \quad , \quad \mathfrak{a} \in \mathfrak{f} \quad \text{gemäß (1.5)} ,$$

einen Charakter von $\check{\mathfrak{K}}_f$ definiert ist. Dies gilt nicht im Fall $\sqrt{-3} \notin \Omega_f$. Hier kann man in jeder Klasse je unendlich viele Vertreter $\mathfrak{a}$ mit $N(\mathfrak{a}) \equiv 1($ bzw. $N(\mathfrak{a}) \equiv -1(3)$ finden. Entsprechendes gilt für $\sqrt{-4}$. Man hat dann

Satz (1.3): Die Erweiterung Ω/Σ sei in Ω_f enthalten. Dann gilt für die Relativnorm $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) = N_{\Omega_f/\Omega}(\varepsilon(\mathfrak{k},\mathfrak{f}))$:

1) $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) \notin \Omega^3 \Rightarrow (\sqrt{-3} \in \Omega$ und $\chi_{-3}(\mathfrak{k}) = \chi_{-3}(\mathfrak{f}) = -1)$

2) $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) \in \Omega^4$

3) $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) \notin \Omega^8 \Rightarrow (\sqrt{-4} \in \Omega$ und $\chi_{-4}(\mathfrak{k}) = \chi_{-4}(\mathfrak{f}) = -1)$

4) Für $e = 3, 8$ gilt

$$\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) , \varepsilon_\Omega(\mathfrak{k}',\mathfrak{f}') \notin \Omega^e \Rightarrow \frac{\varepsilon_\Omega(\mathfrak{k}',\mathfrak{f}')}{\varepsilon_\Omega(\mathfrak{k},\mathfrak{f})} \in \Omega^e .$$

In 3) und 4) gilt auch die Umkehrung, falls $3 \nmid [\Omega_f : \Omega]$ bzw. $2 \nmid [\Omega_f : \Omega]$.

Bevor wir die vorstehenden Sätze im Abschnitt 2 beweisen, kommen wir zu einigen Anwendungen der Sätze (1.1) und (1.3).

Sei $\Omega|\Sigma$ wie in Satz (1.3) eine in Ω_f enthaltene Erweiterung von Σ und E_Ω die Einheitengruppe von Ω. Hierin betrachten wir die Untergruppen

$$(1.12) \qquad U_\Omega = < \{\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) \mid \mathfrak{k},\mathfrak{f} \in \check{\mathfrak{K}}_f\} > ,$$

$$(1.13) \qquad U_\Omega^{\frac{1}{24}} = \{\varepsilon \in E_\Omega \mid \varepsilon^{24} \in U_\Omega\} .$$

Aus Satz (1.3) ergibt sich dann ein einfacher Beweis des folgendes Satzes, dessen erster Teil im Fall $f = 1$ in [5] Theorem (5.1) und für beliebiges f in [3] enthalten ist.

Satz (1.4) Es gibt eine Untergruppe U^*_Ω von $U_\Omega^{\frac{1}{24}}$ mit

$$[E_\Omega : U^*] = c_\Omega \frac{1}{e} \left(\frac{w_\Sigma}{2}\right)^{[\Omega:\Sigma]-1} \frac{[\Omega:\Sigma]}{h_\Sigma} h_\Omega$$

und

$$[U^{\frac{1}{24}} : U^*] \mid ggT(6,[\Omega_f : \Omega]) \quad .$$

Hierin bedeuten h_Ω , h_Σ und w_Ω, w_Σ Klassenzahl und Anzahl der Einheitswurzeln des entsprechenden Körpers. e ist 2 oder 1 je nachdem w_Ω durch 8 teilbar ist oder nicht. c_Ω ist ein explizit angebarer Faktor. Im Fall $f = 1$ ist $c_\Omega = 1$.

Im Fall $f \neq 1$ entsteht c_Ω dadurch, daß man für jeden zu der Erweiterung $\Omega|\Sigma$ gehörigen Charakter $\chi \neq 1$ von $\check{\mathfrak{K}}_f$ mit dem Führer f_χ , $f_\chi \in \mathbb{N}$, die zugehörige L-Funktion durch die Zetafunktionen der Ringidealklassen modulo f ausdrückt (vgl. [6]). Nach [3] ist

$$(1.14) \qquad c_\Omega = \prod_{\chi \neq 1} \left(\frac{f}{f_\chi} \sum_{\substack{f_1, f_2 \in \mathbb{N} \\ f_1 f_2 = f \\ f_\chi | f_1}} \frac{[\Omega_f : \Omega_{f_\chi}]}{f_2^2} \prod_{\mathfrak{p} | f_1} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})}\right) \right)$$

oder auch mit den in [15] definierten Zahlen $G(p^{n_p(\chi)}, \chi)$:

$$(1.15) \qquad c_\Omega = \prod_{\chi \neq 1} G(p^{n_\chi(p)}, \chi)$$

wobei jeweils das Produkt über alle zur Erweiterung Ω/Σ gehörigen Charaktere $\chi \neq 1$ zu erstrecken ist. $\mathfrak{p}$ durchläuft die Primidealteiler von f_1 in Σ .

Der hier gegebene Beweis von Satz (1.4) beruht auf der gegenüber [3] und [5] genaueren Beschreibung von $U_\Omega^{\frac{1}{24}}$ und kommt ohne die komplizierten Überlegungen in [5], S. 218-223, die auch in [3] benutzt werden, aus.

Die durch die beiden folgenden Sätze gelösten Probleme wurden mir von Herrn Sczech mitgeteilt. Eine Anwendung von Satz (1.1) ist zunächst

Satz (1.5) Sei $d_\Sigma \not\equiv -3, -4$ und β Basisquotient eines eigentlichen Ideals von $\mathfrak{O}_f$. Dann gibt es eine Einheit ε in Ω_f mit

$$\varepsilon j(\beta) \in \Omega_f^3$$

und $$\varepsilon(j(\beta) - 12^3) \in \Omega_f^2 .$$

Im Fall $d_\Sigma \equiv 1(8)$ ist eine solche Einheit ε von Herrn Sczech aus dem in [17] enthaltenen Formelmaterial gefunden worden. Der in Abschnitt 2 gegebene Beweis zeigt, wie man im allgemeinen Fall ε aus den Einheiten $E(\mathfrak{a}, \mathfrak{b})$ konstruieren kann. Es sei an dieser Stelle noch bemerkt, daß $j(\beta)$ nicht immer ein Kubus und $j(\beta) -12^3$ nicht immer ein Quadrat in Ω_f ist (vgl. [13]).

Aus Satz (1.5) folgt

Satz (1.6): Sei $d_\Sigma \not\equiv -3, -4$ und $\mathfrak{a}$ ein eigentliches Ideal von $\mathfrak{O}_f$. Dann gibt es eine Zahl ξ in $\mathbb{C}$, so daß die zum Gitter $\mathfrak{w} = \xi\mathfrak{a}$ gehörige elliptische Kurve in Weierstraß-Normalform

$$y^2 = 4x^3 - g_2(\mathfrak{w})x - g_3(\mathfrak{w})$$

ganze Koeffizienten in Ω_f und außerhalb von 2 und 3 gute Reduktion hat.

2. Beweise der Sätze (1.1) - (1.6)

Zu Satz (1.1): Grundlegend für das folgende ist die Transformationsformel der Dedekindschen η-Funktion. Für eine unimodulare Matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gilt bekanntlich mit einer 24-ten Einheitswurzel $\varepsilon(M)$

$$\eta(Mz) = \varepsilon(M) \sqrt{cz+d} \;\; \eta(z) , \tag{2.1}$$

wobei die Wurzel mit positivem Realteil zu nehmen ist. Für $\varepsilon(M)$ hat man nach [7] die Darstellung

$$\varepsilon(M) = \left(\frac{a}{c_1}\right) \zeta_{24}^{\,ab+c(d(1-a^2)-a) + 3(a-1)c_1 + \lambda \frac{3}{2}(a^2-1)} \tag{2.2}$$

sofern $c \geq o$ und $d > o$ im Fall $c = o$ ist. c_1 und λ entstehen aus der Zerlegung $c = c_1 2^{\lambda}$, $2 \nmid c_1$, von c im Fall $c > o$, und im Fall $c = o$ ist $c_1 = 1$, $\lambda = o$ zu setzen. $(\frac{a}{c_1})$ bedeutet das Legendresymbol im Fall $a \neq o$ und 1 im Fall $a = o$. Für $n \in \mathbb{N}$ ist dabei $\zeta_n = e^{\frac{2\pi i}{n}}$.
Wir benötigen weiter noch die Funktionen

$$(2.3) \qquad \gamma_2(z) = \sqrt[3]{j(z)} = 12 \frac{g_2(z)}{(2\pi)^4 \eta(z)^8}$$

$$(2.4) \qquad \gamma_3(z) = \sqrt{j(z)-12^3} = 6^3 \frac{g_3(z)}{(2\pi)^6 \eta(z)^{12}}$$

Hierfür hat man die Transformationsformeln

$$(2.5) \qquad \gamma_2(Mz) = \varepsilon(M)^{-8} \gamma_2(z)$$

$$(2.6) \qquad \gamma_3(Mz) = \varepsilon(M)^{-12} \gamma_3(z)$$

für jede unimodulare Matrix M.

Im Hinblick auf (1.10) betrachten wir nun für zwei zu 6 teilerfremde ganze Zahlen p,q die Funktion

$$(2.7) \qquad F(z) = \frac{\eta(\frac{z}{pq})\,\eta(z)}{\eta(\frac{z}{p})\,\eta(\frac{z}{q})}$$

Für eine unimodulare Matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit $b \equiv o(pq)$ ergibt sich dann aus (2.2) die Transformationsformel

$$(2.8) \qquad F(Mz) = \zeta_6^{[a\frac{b}{pq} + c(d(1-a^2)-a) + 3(a-1)c_1]\frac{p-1}{2}\,\frac{q-1}{2}} F(z).$$

$$(2.9) \qquad \gamma_2(Mz)\,\gamma_3(Mz) = \zeta_6^{[ab + c(d(1-a^2)-a) + 3(a-1)c_1]} \gamma_2(z)\gamma_3(z).$$

Die Funktion

$$(2.10) \qquad h(z) = \frac{(\gamma_2(z)\gamma_3(z))^{\frac{p-1}{2}\,\frac{q-1}{2}}}{F(z)}$$

hat daher die Transformationsformel

$$(2.11) \qquad h(Mz) = \zeta_6^{\,a[b - \frac{b}{pq}]\,\frac{p-1}{2}\,\frac{q-1}{2}}\; h(z)$$

wenn $b \equiv o(pq)$ ist.

Der bei ζ_6 auftretende Exponent ist nun wegen $(pq,6) = 1$ stets durch 6 teilbar. Folglich ist h eine zur Untergruppe $\Gamma^0(pq)$ von $SL_2(\mathbb{Z})$ gehörige Modulfunktion, die außerdem in der oberen Halbebene holomorph ist. Daher gilt

$$(2.12) \qquad h(z) = R\left(j(z)\,,\ \frac{\Delta\binom{z}{pq}}{\Delta\binom{z}{1}}\right)$$

mit einer rationalen Funktion R, deren Koeffizienten nach dem q-Entwicklungsprinzip rational sind. Der Nenner läßt sich schreiben als das Produkt

$$(2.13) \qquad \prod_{S \nmid \left(\begin{smallmatrix}1 & o\\ o & pq\end{smallmatrix}\right)} \left(\frac{\Delta\binom{z}{pq}}{\Delta\binom{z}{1}} - \frac{\Delta\left(S\binom{z}{1}\right)}{\Delta\binom{z}{1}}\right)\ ,$$

in dem S ein Vertretersystem von zu $\left(\begin{smallmatrix}1 & o\\ o & pq\end{smallmatrix}\right)$ inäquivalenten primitiven Matrizen der Determinante pq durchläuft (vgl. [1]). (2.12) gilt auch für den Funktionswert an der Stelle $z = \alpha$, sofern der Nenner hier keine Nullstelle hat. Letzteres folgt aber aus (2.13), unter Beachtung der in [1] bestimmten Faktorisierung dieser Zahlen:

$$(2.14) \qquad (pq)^{12}\,\frac{\Delta\binom{\alpha}{pq}}{\Delta\binom{\alpha}{1}} \approx (\bar{\mathfrak{p}}\mathfrak{q})^{12}$$

$$(pq)^{12}\,\frac{\Delta\left(S\binom{\alpha}{1}\right)}{\Delta\binom{\alpha}{1}} \approx (\mathfrak{p}\bar{\mathfrak{q}})^{12} \qquad \text{falls } S \nmid \left(\begin{smallmatrix}1 & o\\ o & pq\end{smallmatrix}\right)$$

und $S\binom{\alpha}{1}$ Basis von $\bar{\mathfrak{p}}_f\,\mathfrak{q}_f$ ist,

$$(pq)^{12}\,\frac{\Delta\left(S\binom{\alpha}{1}\right)}{\Delta\binom{\alpha}{1}} \not\approx \bar{\mathfrak{p}}\mathfrak{q},\ \mathfrak{p}\bar{\mathfrak{q}} \qquad \text{sonst}$$

und der Tatsache, daß $\mathfrak{p} \neq \bar{\mathfrak{q}}$ vorausgesetzt worden ist. Also gilt

$$(2.15)\qquad h(\alpha) = R\left(j(\alpha)\,,\ \frac{\Delta(\mathfrak{a}\bar{\mathfrak{b}})}{\Delta(\mathfrak{o}_f)}\right) \in \Omega_f\,.$$

Weiterhin hat man nach [13]

$$(2.16)\qquad \Omega_f(\gamma_2(\alpha)) = \begin{cases} \Omega_{3f} & \text{falls} \quad 3 \mid f^2 d_\Sigma \\ \Omega_f & \text{falls} \quad 3 \nmid f^2 d_\Sigma \end{cases}$$

und

$$(2.17)\qquad \Omega_f(\gamma_3(\alpha)) = \begin{cases} \Omega_{2f} & \text{falls} \quad 2 \mid f^2 d_\Sigma \\ \Omega_f & \text{falls} \quad 2 \nmid f^2 d_\Sigma \end{cases} .$$

Satz (1.1) folgt nun aus (2.15), (2.16) und (2.17). Beim Beweis des zweiten Teils beachte man, daß für das in der Definition von $E(\mathfrak{a}',\mathfrak{b}')$ auftretende α' wegen Spur $(\alpha) \equiv$ Spur $(\alpha') \equiv 0 \mod 12$ auch $\alpha' = \alpha + 6\mu$, $\mu \in \mathbb{Z}$, ist und somit $\gamma_2(\alpha') = \gamma_2(\alpha)$ und $\gamma_3(\alpha') = \gamma_3(\alpha)$ gelten muß.

Zu Satz (1.2): Es genügt

$$(2.18)\qquad h(\alpha)^{\sigma(\mathfrak{q}_0)} = h\left(\frac{\alpha}{q_0}\right),$$

$$(2.19)\qquad \gamma_2(\alpha)^{\sigma(\mathfrak{q}_0)} = \gamma_2\left(\frac{\alpha}{q_0}\right),$$

$$(2.20)\qquad \gamma_3(\alpha)^{\sigma(\mathfrak{q}_0)} = \gamma_3\left(\frac{\alpha}{q_0}\right)$$

zu beweisen. (2.18) folgt aus (2.15) unter Beachtung von (1.3) und der bekannten Tatsache, daß $j(\alpha)^{\sigma(\mathfrak{q}_0)} = j\left(\frac{\alpha}{q_0}\right)$ ist. Der Beweis von (2.19) und (2.20) ergibt sich aus [13] wenn man auf die dortigen Darstellungen (5.1) die Fortsetzungen $\sigma([q_0, 3\alpha]^{-1})$ bzw. $\sigma([q_0, 2\alpha]^{-1})$ von $\sigma(\mathfrak{q}_0)$ auf Ω_{3f} bzw. Ω_{2f} anwendet. Man kann Satz (1.2) aber auch mit Hilfe des Reziprozitätsgesetzes von Stark ([16], Theorem 3') ohne den Umweg über γ_2 und γ_3 beweisen, weil im vorliegenden Fall die in [16] auftretende Matrix B die einfache Gestalt $B = \begin{pmatrix} 1 & 0 \\ 0 & q_0 \end{pmatrix}$ hat. Es sei an dieser Stelle noch bemerkt, daß man beim Versuch, den Satz (1.1) mit Hilfe von [16] zu beweisen, auf erhebliche Schwierigkeiten stößt.

Zu Satz (1.3): Sei $\mathfrak{U}$ die zu der Erweiterung Ω/Σ gehörige Untergruppe von $\breve{\mathfrak{K}}_f$. Dann folgt aus (1.3) zunächst, daß die Relativnorm $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f})$ nur von den Nebenklassen $\mathfrak{k}\mathfrak{U}$ und $\mathfrak{f}\mathfrak{U}$ abhängt.

Zu 1): Ist $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) \notin \Omega^3$, so muß wegen Satz (1.1) $N(\mathfrak{a}) \equiv N(\mathfrak{b}) \equiv -1(3)$ für jedes Paar $\mathfrak{a},\mathfrak{b}$ von gemäß (1.5) gewählten Vertretern von $\mathfrak{k}\mathfrak{A}$ und $\mathfrak{f}\mathfrak{A}$ gelten. Durch (1.11) ist daher ein Charakter χ_{-3} von $\mathfrak{K}_f/\mathfrak{A}$ definiert und es gilt $\chi_{-3}(\mathfrak{k}) = \chi_{-3}(\mathfrak{f}) = -1$. Da ferner χ_{-3} gleich dem zu der Erweiterung $\Sigma(\sqrt{-3})/\Sigma$ gehörigen Charakter ist (vgl. [12]), muß weiter $\Sigma(\sqrt{-3}) \subseteq \Omega$, also $\sqrt{-3} \in \Omega$ sein.

Im Fall $3 \nmid [\Omega_f:\Omega]$ folgt die Umkehrung von 1) so: Es ist

$$(2.22) \qquad \sqrt[3]{\varepsilon_\Omega(\mathfrak{k},\mathfrak{f})} = \prod_{\phi \in \mathrm{Aut}(\Omega_f/\Omega)} E(\mathfrak{a},\mathfrak{b})^{8\hat{\phi}}$$

wobei $\hat{\phi}$ irgendeine Fortsetzung von ϕ auf Ω_{3f} bedeutet. Wegen Satz (1.1) gibt es einen Automorphismus ϕ_0 von Ω_{3f}/Ω_f mit $E(\mathfrak{a},\mathfrak{b})^{\phi_0-1} = \zeta_3$, und aus (2.22) folgt dann wegen $\hat{\phi}\phi_0 = \phi_0\hat{\phi}$, $\zeta_3{}^{\phi_0} = \zeta_3$

$$(2.23) \qquad \sqrt[3]{\varepsilon_\Omega(\mathfrak{k},\mathfrak{f})}^{\,\phi_0-1} = \zeta_3^{[\Omega_f:\Omega]}$$

und damit $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) \notin \Omega^3$, wobei $\zeta_3 \in \Omega$ zu beachten ist.

Zu 2): $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f}) \in \Omega^4$ folgt unmittelbar aus Satz (1.1).

Zu 3): Diese Behauptung folgt analog zu 1) aus Satz (1.1).

Zu 4): Dies ergibt sich aus 1), 3) und Teil 3 von Satz (1.1).

<u>Zu Satz (1.4):</u> Ausgangspunkt ist die Formel

$$(2.24) \qquad [E_\Omega : \mu_\Omega U_\Omega] = (12 w_\Sigma)^{[\Omega:1]-1} \, \frac{w_\Sigma}{w_\Sigma} \cdot c_\Omega \, \frac{[\Omega:\Sigma]}{h_\Sigma} \, h_\Omega$$

die man im wesentlichen aus der Kroneckerschen Grenzformel für die zu der Erweiterung Ω/Σ gehörigen L-Funktion gewinnt [6]. μ_Ω bezeichnet dabei die in Ω enthaltene Gruppe der Einheitswurzeln. Im Fall $f = 1$ ist diese Herleitung in [5], Theorem (3.4) enthalten, und im Fall $f \neq 1$ verläuft dies völlig analog.

Wir setzen zur Abkürzung

(2.25) $n := [\Omega:\Sigma]$, $m = [\Omega_f:\Sigma]$, $i := [\mu_\Omega U_\Omega : U_\Omega^{\frac{1}{24}}]$

und zeigen, gestützt auf Satz (1.3) die Teilbarkeitsbeziehungen:

(2.26)
$$24^{n-1} \mid i \mid 24^{n-1} \quad , \text{ falls } \sqrt{-3} \notin \Omega , \ \sqrt{-4} \notin \Omega$$
$$\frac{1}{3}\, 24^{n-1} \mid i \mid \frac{(3,m)}{3}\, 24^{n-1} \quad , \text{ falls } \sqrt{-3} \in \Omega , \ \sqrt{-4} \notin \Omega$$
$$\frac{1}{2}\, 24^{n-1} \mid i \mid \frac{(2,m)}{2}\, 24^{n-1} \quad , \text{ falls } \sqrt{-3} \notin \Omega , \ \sqrt{-4} \in \Omega$$
$$\frac{1}{6}\, 24^{n-1} \mid i \mid \frac{(6,m)}{6}\, 24^{n-1} \quad , \text{ falls } \sqrt{-3} \in \Omega , \ \sqrt{-4} \in \Omega$$

Aus (2.23) folgt dann Satz (1.2) und der Zusatz (1.16), wobei zu beachten ist, daß der Geschlechterkörper von Ω nach [1] vom Typ (2,2,...) ist und somit μ_Ω immer eine Untergruppe der 24-ten Einheitswurzel sein muß.

Zum Beweis von (2.26) unterscheiden wir die dort angegebenen Fälle:
Im Fall $\sqrt{-3} \notin \Omega$, $\sqrt{-4} \notin \Omega$ ist nach Satz (1.3) jedes Element aus U_Ω eine 24-te Potenz in E_Ω und somit $i = 24^{n-1}$, da der Einheitenrang von Ω gleich $n - 1$ ist. Im Fall $\sqrt{-3} \in \Omega$, $\sqrt{-4} \notin \Omega$ gehen wir von einer in U_Ω enthaltenen Basis $\varepsilon_1,\dots,\varepsilon_{n-1}$ von U_Ω modulo μ_Ω aus. Wegen $\sqrt{-4} \notin \Omega$ ist dann nach Satz (1.3) jedes ε_i eine 8-te Potenz in E_Ω , also

(2.27) $8^{n-1} \mid i \mid 24^{n-1}$.

Wir betrachten nun die beiden Fälle

a) Jedes ε_i ist eine 3-te Potenz in E_Ω .
b) Ein ε_i ist keine 3-te Potenz in E_Ω .

Im Fall a) hat man

(2.28) $3^{n-1} \mid i$,

nach Satz (1.3) ist in diesem Fall notwendig $(3,m) = 3$ und aus (2.27) und (2.28) folgt nun (2.26).

/ /

Im Fall b) seien ohne Einschränkung genau $\varepsilon_1,\dots,\varepsilon_t$ keine 3-te Potenz in Ω . Nach Satz (1.3), 4) erzeugen dann ihre 3-ten Wurzeln über Ω denselben Körper und es folgt, daß mit geeigneten Exponenten $\nu_i = \pm 1$:

$$(2.29) \qquad \varepsilon_i \varepsilon_1^{\nu_i} \in \Omega^3 \qquad i = 2,\dots,t .$$

Es gibt also eine Basis von U_Ω in der genau eine Einheit keine 3-te Potenz in Ω ist. Daraus folgt

$$(2.30) \qquad \frac{1}{3}\, 3^{n-1} \mid i .$$

Im Fall $(3,m) = 3$ ergibt sich hieraus in Verbindung mit (2.27) die Behauptung von (2.26). Im Fall $(3,m) = 1$ folgt aus Satz (1.3), daß ein $\varepsilon_\Omega(\mathfrak{k},\mathfrak{f})$ und damit mindestens ein ε_i keine 3-te Potenz in Ω ist und somit

$$(2.31) \qquad i \mid \frac{1}{3} \cdot 24^{n-1}$$

gelten muß. (2.26) ergibt sich nun aus (2.30) und (2.31). Damit ist (2.26) in den ersten beiden Fällen bewiesen. In den beiden letzten Fällen beweist man (2.26) analog.

Zu Satz (1.5): Da $j(\beta)$ zu $j(\alpha)$ konjugiert ist, genügt es, die Behauptung für $\beta = \alpha$ zu beweisen. Hierzu wähle man in Σ zwei Primideale ersten Grades $\mathfrak{p}$ und $\mathfrak{q}$ der Norm p und q mit $p \neq q$, $ggT(pq,6f) = 1$, $p \equiv q \equiv -1(4)$, $p \equiv q \equiv -1(3)$. Dies ist möglich, weil wir $d_\Sigma \neq -3, -4$ vorausgesetzt haben. Aus dem Beweis zu Satz (1.1) folgt dann

$$(2.32) \qquad E(\mathfrak{p},\mathfrak{q})\,(\gamma_2(\alpha)\gamma_3(\alpha))^{-\frac{p-1}{2}\frac{q-1}{2}} \in \Omega_f .$$

Da $\frac{p-1}{2}\frac{q-1}{2}$ zu 6 teilerfremd ist, liefert Potenzieren mit $-6\frac{p-1}{2}\frac{q-1}{2}$, daß

$$(2.33) \qquad E(\mathfrak{p},\mathfrak{q})^{-6\frac{p-1}{2}\frac{q-1}{2}}\, j(\alpha)^2(j(\alpha) - 12^3)^3$$

eine 6-te Potenz in Ω_f ist. Die Einheit

$$(2.34) \qquad \varepsilon = E(\mathfrak{p},\mathfrak{q})^{-6\frac{p-1}{2}\frac{q-1}{2}}$$

leistet also das Verlangte.

<u>Zu Satz (1.6):</u> Sei $\lambda \in \mathbb{C}$, $\lambda^{12} = \dfrac{\varepsilon}{\Delta(\mathfrak{w})}$ mit ε aus Satz (1.5). Dann gilt für $\mathfrak{m}\Omega = (6\lambda)^{-1}\mathfrak{w}$:

(2.35) $$g_2(\mathfrak{m}\Omega) = 3\cdot 36\,\sqrt[3]{\varepsilon j(\mathfrak{w})}$$

$$g_3(\mathfrak{m}\Omega) = 6\,\sqrt{\varepsilon(j(\mathfrak{w})-12^3)}\quad ,$$

wobei λ gegebenenfalls noch um eine 3-te Einheitswurzel so abzuändern ist, daß die 3-te Wurzel in (2.35) in Ω_f liegt. Man berechnet dann

(2.36) $$\Delta(\mathfrak{m}\Omega) = g_2(\mathfrak{m}\Omega)^3 - 27\, g_3(\mathfrak{m}\Omega)^2 = 6^{12}\,\varepsilon\quad ,$$

womit alles gezeigt ist.

Literatur

[1] Deuring, Die Klassenkörper der komplexen Multiplikation, Enzykl. d. Math. Wiss., Bd. I/2, Heft 10, Teil II.

[2] Gras, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unitées des extensions abéliennes réelles de $\mathbb{Q}$, Bull. Sci. Math. (2), 101 (1977), 97 - 129.

[3] Hayashi, Note on an index formula of elliptic units in a ring class field.

[4] Kronecker, Werke Bd. IV.

[5] Kubert-Lang, Modular units, Grundlehren der Math. Wiss. 244, Springer 1981.

[6] Meyer, Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern, Akademie Verlag Berlin 1957.

[7] Meyer, Über einige Anwendungen Dedekindscher Summen, J. Reine u. Angew. Math. 198 (1957), 143-203.

[8] Nakamula, Class number calculation of a cubic field from the elliptic unit, J. Reine u. Angew. Math., 331 (1982), 114-123.

[9] Nakamula, Class number calculation of a quartic field from the elliptic unit, Acta Arithmetica 45.

[10] Nakamula, Class number calculation of a sextic field from the elliptic unit, Acta Arithmetica 45.

[11] Robert, Unitées elliptiques, Bull. Soc. Math. France, Mém. No. 36, Paris 1973.

[12] Schertz, L-Reihen in imaginär-quadratischen Zahlkörpern und ihre Anwendung auf Klassenzahlprobleme bei quadratischen und biquadratischen Zahlkörpern, I,II J. Reine u. Angew. Math. 262/63 (1973), 120-133, 270 (1974), 195-212.

[13] Schertz, Die singulären Werte der Weberschen Funktionen f, f_1, f_2, γ_2, γ_3 J. Reine u. Angew. Math. 286/87 (1976), 46-74.

[14] Schertz, Die Klassenzahl der Teilkörper abelscher Erweiterungen imaginär-quadratischer Körper I,II, J. Reine u. Angew. Math. 295 (1977) 151-168; 296 (1977), 60-79.

[15] Schertz, Zur Theorie der Ringklassenkörper über imaginär-quadratischen Zahlkörpern, Journal of Number Theory, Vol. 10, No. 1 (1978).

[16] Stark, L-functions at s = 1, IV, Advances in Math. 35 (1980), 197-235.

[17] Weber, Lehrbuch der Algebra III.